

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (Currently amended) A memory device storing a data structure for
2 tracking network behavior, comprising:
3 | a connection table that maps each node of a network to a record ~~object~~ that
4 stores information about traffic to or from the node and between that node and
5 others nodes in the network.

1 2. (original) The device of claim 1 wherein the connection table includes a
2 plurality of records that are indexed by source address.

1 3. (original) The device of claim 1 wherein the connection table includes a
2 plurality of records that are indexed by destination address.

1 4. (original) The device of claim 1 wherein the connection table includes a
2 plurality of records that are indexed by time.

1 5. (Currently amended) The device of claim 1 wherein the connection
2 | table includes a plurality of records, that are record objects, which ~~that~~ are
3 indexed by source address, destination address and time.

1 6. (original) The device of claim 1 wherein the connection table is a
2 plurality of connection sub-tables each sub-table having data pertaining to
3 network traffic over different time scales.

1 | 7. (Currently amended) The device of ~~claim 1~~ claim 6 wherein the
2 connection sub-tables include a time-slice connection table that operates on a
3 small unit of time and at least one other sub-table that operates on a larger unit of
4 time than the time slice sub-table.

1 8. (original) The device of claim 7 wherein the at one sub-table holds
2 records received from all collectors over the time scale of the table.

1 9. (original) The device of claim 5 wherein the addresses indexing the
2 connection table are IP addresses.

1 10 (Previously presented) The device of claim 1 wherein the addresses
2 indexing the connection table include a physical layer address to IP address map
3 that is used to determine Host ID.

1 11. (Currently amended) The device of claim 1 wherein the host record of
2 a first host maps that first host to a second host that communicates with the first
3 host to a `[[["]]host pair record object[["]]` that has information about all the traffic
4 from the first to the second host and from the second host to the first host.

1 12. (Previously presented) The device of claim 1 wherein the connection
2 table includes two level mapping that enables a consuming device to obtain
3 summary information about one host for a first level mapping and about the
4 traffic between any pair of hosts, in either direction, between a first one of the
5 hosts of the any pair to a second one of the hosts of the any pair and from the
6 second one of the hosts of the any pair to the first one of the hosts of the any pair
7 for a second level mapping.

1 | 13. (Currently amended) The device of claim 1 wherein the connection
2 | table comprises a plurality of host records, a host record stores a measure of the
3 | number of bytes, packets, and connections that occurred between hosts during a
4 | given time-period.

1 | 14. (Currently Amended) The device of ~~claim 1~~ claim 13, wherein data in
2 | the host record is organized by well known transport protocols and well-known
3 | application-level protocols.

1 | 15. (Currently Amended) The device of ~~claim 1~~ claim 13, wherein host
2 | records have no specific memory limit.

1 | 16. (original) The device of claim 1 wherein for application-level
2 | protocols and for every pair of hosts, the connection table stores statistics for
3 | traffic between the hosts.

1 | 17. (original) The device of claim 16 wherein the connection table stores
2 | protocol-specific records as (protocol, count) key-value pairs.

1 | 18. (New) A memory device storing a data structure for tracking network
2 | behavior, the data structure comprising:
3 | a connection table that maps each node of a network to a record that stores
4 | connection information about traffic to or from the node and between that node
5 | and others nodes that have connections with the node in the network, the
6 | connection table indexed according to at least a first one of source address,
7 | destination address and time;
8 | the connection table further including in the records fields for storing
9 | statistical information for traffic between the hosts.

1 19 (New) The device of claim 18 wherein the plurality of records is record
2 objects.

1 20. (New) The device of claim 18 wherein the connection table is a second
2 plurality of connection sub-tables, each sub-table having data pertaining to
3 network traffic over different ones of corresponding second plurality of time
4 scales.

1 21. (New) The device of claim 18 wherein the connection sub-tables
2 include a time-slice connection table that operates on a small unit of time and at
3 least one other sub-table that operates on a larger unit of time than the time slice
4 sub-table.

1 22. (New) The device of claim 18 wherein the at one sub-table holds
2 records received from all collectors in the network over the time scale of the
3 table.

1 23. (New) The device of claim 18 wherein the addresses indexing the
2 connection table are IP addresses.

1 24. (Currently amended) The device of claim 23 wherein the addresses
2 indexing the connection table include a physical layer address to IP address map
3 that is used to determine Host ID.
4

5 25. (New) The device of claim 18 wherein the host record of a first host
6 maps that first host to a second host that communicates with the first host to a
7 host pair record that has information about all the traffic from the first to the
8 second host and from the second host to the first host.

1 26. (New) The device of claim 18 wherein the connection table includes
2 two level mapping that enables a consuming device to obtain summary
3 information about one host for a first level mapping and about the traffic between
4 any pair of hosts, in either direction, between a first one of the hosts of the any
5 pair to a second one of the hosts of the any pair and from the second one of the
6 hosts of the any pair to the first one of the hosts of the any pair for a second level
7 mapping.

1 27. (New) The device of claim 18 wherein the connection table comprises
2 a plurality of host records, a host record stores, a measure of the number of bytes,
3 packets, and connections that occurred between hosts during a time-period.

1 28. (New) The device of claim 27 wherein data in the host record is
2 organized by well known transport protocols and well-known application-level
3 protocols.

1 29. (New) The device of claim 28 wherein for application-level protocols
2 and for every pair of hosts, the connection table stores statistics for traffic
3 between the hosts.

1 30 (New) The device of claim 28 wherein the connection table stores
2 protocol-specific records as (protocol, count) key-value pairs.